Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

MEMORANDUM FOR THE RECORD

SUBJECT: Computer Security Training--Working Group Report to the DCI Computer Security Subcommittee

The objectives of the working group were to survey existing computer security course offerings, to determine intelligence community applicability, and to examine the utility of requesting modification to current course curricula in light of perceived subcommittee instructional requirements.

The previous review (See Attachment #1) by the State Department member, in response to Chairman Tasking, provided an excellent baseline for working group consideration. Our own examination of the updated course offerings revealed nothing that would require modifications to the commonality analysis performed in the Department of State-conducted review.

A survey, the results of which are detailed in Attachment #2, was conducted among community members and instructional agencies. It is apparent from the survey and subsequent discussions that the bulk of the community was not aware of the nature or availability of the NSA-sponsored training. This is perhaps due to the cryptologic name associated with the training activity. Whatever the reason, we feel the course is of considerable value and warrants increased community participation.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Due to the constraints on participation at the Ft. Lee facility and the classification limitations of the DODCI training, and the limited scope of other available training, it is recommended that the NSA course be utilized as the prime source of intelligence community computer security training.

If the target audience requests that the training be conducted other than on-site NSA, this subcommittee will negotiate with NSA in order to effect that alternate site training. It is further recommended that desired course additions, if any, be proposed and justified (and perhaps funded) by individual activities (i.e., Army, Navy, Air Force, etc.).

Limited topic, executive level training is currently available from DODCI. Curricula structure is tailored to the target audience and can be conducted within the trainees' own facility. Non-DOD activities must pay a nominal fee for such training.

Attachments 3, 4, 5 provide curricula detail.

Attachments:
1. Review of Lesson Plans for Comp. Security Courses
2. Computer Security Training
3. NSA Course
4. DODCI Special/On-site ADP Courses
5. Computer System Security Course

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

UNCLASSIFIED

DEPARTMENT OF STATE

Washington, D.C. 20520

8 September 1977

STAT TO: [redacted] Chairman
DCI Computer Security Subcommittee
National Security Agency
Fort Meade, Maryland 20755

FROM: Mr. George S. Herrmann, State Member GSH
DCI Computer Security Subcommittee
U.S. Department of State
Washington, D.C. 20520

SUBJ: Review of Existing Lesson Plans for Computer Security Courses

During the week of August 29 through September 2 1977, I reviewed three lesson plans developed for computer security training courses. These courses are taught by the National Security Agency at Ft. Meade, by the U.S. Army Logistics Management Center at Ft. Lee, Virginia, and by the Department of Defense Computer Institute in Washington, D.C. The objective of my study was to determine the degree to which these courses overlap, and to glean from the overlap a basic structure for a course in computer security which might be established for interagency participation under the auspices of the Computer Security Subcommittee.

As might be expected, there were a number of topics common to all three courses: these are listed in Annex A. Several topics were common to two of the three courses; these appear in Annex B. Some topics were unique to each course: I found these to be the most interesting topics, and have included them in Annex C.

The DODCI course is a four-day offering, aimed apparently at mid-level management. The NSA and Ft. Lee courses last, respectively, one week and two weeks. These relatively long course times allow student resolution of class problems at NSA and problem workshops at Ft. Lee. These practical exercises strike me as valuable training tools which help reinforce security practices presented in the lecture courses.

Ft. Lee brings in guest speakers from private industry to lecture on the strengths and weaknesses of various computer systems. I was unable to determine whether Ft. Meade does this or not, but I forsee some scheduling problems with this approach.

UNCLASSIFIED

Atch #1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

The Ft. Lee course features 5 1/2 hours of instruction on computer fraud. It is my opinion that this course might be of interest to the Department of the Treasury and FBI representatives to the Subcommittee, if they have not already taken the course.

Conclusions: The Ft. Lee and DODCI courses are open to personnel from other government agencies on a space available basis; this is presumably true of the course at NSA. The existing courses seem adequate: I believe that it would be premature at this point to establish a separate interagency computer security course unless there are important topics of concern to us which are not taught by the existing schools. I suspect that there are additional computer security courses available at other government agencies of which I am presently unaware, and that the cirreculums for these courses should be reviewed before we consider establishing a new course geared expressly to the needs of the Intelligence Community.

I do recommend that Annex A to this paper, listing topics common to the three courses I examined, should serve as a starting point for any computer security course we consider creating. I would also suggest that the administrative office for each of the three schools be asked to keep the Chairman, CSS informed of their projected class schedules, so that Subcommittee members may propose personnel for these courses in advance of course starting dates.

With the permission of the Chairman, I will continue to make the rounds of government agencies offering computer security courses in an effort to compile a more complete list of course offerings. When I have what I feel is a complete list, I will again compare cirreculums. I would hope that the Subcommittee, in reviewing the final list of course offerings, can uncover areas of concern to the Intelligence Community that are not offered by an existing school. In my opinion, we should then pursue topics of concern to us for which no instruction is currently available.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

TOPICS COMMON TO ALL THREE COURSES

Course Orientation
Documentation Guidelines, Regulations and Requirements
Computer Security Analysis and Design
Physical Security Considerations
Personnel Security Considerations
Privacy Act Requirements
Computer System Auditing
Data Base Integrity
Commencement Exercises

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

TOPICS COMMON TO TWO COURSES

TOPIC	OFFERING AGENCIES
Security Planning and Management	Ft. Lee & DODCI
Contingency Planning	Ft. Lee & DODCI
Computer Networks	Ft. Lee & DODCI
Data Encryption	Ft. Lee & NSA
Terminal Security Considerations	Ft. Lee & NSA
Hardware and Software Security Considerations	Ft. Lee & NSA
Security Design Principles	Ft. Lee & NSA
Security Kernels	Ft. Lee & NSA
Tempest Considerations	Ft. Lee & NSA

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

ANNEX C

UNIQUE TOPICS

TOPIC	OFFERING AGENCY
COMSEC/EMSEC Considerations	NSA
ADP Accreditation Guidelines	NSA
Authentication	NSA
Authorization	NSA
Logging	NSA
ADP Security Problems	NSA
Mathematical Models	NSA
Review	NSA
Final Exam	NSA
Guest Speakers from Private Industry	Ft. Lee
DOD Computer Systems	Ft. Lee
Physical/Personnel Security Workshop	Ft. Lee
Data Communications Concepts	Ft. Lee
Output Products Security	Ft. Lee
Design of Personnel Security Systems	Ft. Lee
Fraud Considerations, Prevention and Detection	Ft. Lee
Design of Maximum Secure Fraud-Proof Systems	Ft. Lee

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

COMPUTER SECURITY TRAINING

1. NSA - MP-181, Introduction to Computer Security. Presently, it is taught twice a week, two hour sessions, for 9 weeks. The course is being condensed into a one-week course. See attachment for course outline. Contact is [redacted], 342/688-6015. STAT

2. CIA - None, but willing to participate in setting up one. Their people are sent to IBM for training. Paul recommended that the course take place [redacted] with IC staffing. STAT

3. DIA - None, but use cassettes for in-house training, particularly for DIAOLS. Other training: they attend the DODCI Course.

4. DODCI - Offers a 3-day (Tues., Wed., & Thurs.) at Anacostia--Computer Systems Security Course (CS). See attachment for course outline. Contact is Mr. Losonsky, 433-2803.

5. Army - None, attend DODCI Course. There is a course given at Ft. Lee but it is strictly for DARCOM. See attachment.

6. USSS - None

7. FBI - None

8. Navy - None, Attend DODCI Course

9. Air Force - None, Attend DODCI Course

10. ERDA - None

11. State - None

12. CSC - Computer Security Courses deal with Privacy and Freedom of Information Acts.

13. WMCCS - Nine-day workshops in Mississippi have been discontinued. The course has been taken over by DODCI.

Atch #2

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

NSA COURSE

MP-181, Introduction to Computer Security

Presently, it is taught twice a week, two hour sessions, for nine weeks. The course is being condensed into a one week course.

Plan of Instruction

I. Introduction (History of Computer Security and Background Information--GAO and OMB documents, risk analysis)

II. Pertinent DOD, IC and NSA Documents
DCID 1/16
DOD 5200.28
DOD 5200.28-M
NSA/CSS 10-27
NACSEM 7002
Public Law 93-579 (Privacy Act)
CISR 6/3 (Annex E)
USSID 701
Industrial Security Manual

III. Areas of Computer Security Other than Hardware/ Software Security
COMSEC
EMSEC
Physical Security
Personnel Security
Administrative and Operational Controls
NSA/CSS Computer Security Standards

IV. ADP Accreditation Guidelines
ADP Security Design Goals and Standards

V. Tempest Threat

VI. Tempest Tour

VII. Definitions, Design Principles
Definitions (PP1-2, 98-101 Hoffman)
Security Design Principles

VIII. Authentication
Lecture 1
Lecture 2

A.1 #3

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

IX. Authorization
Lecture 1
Lecture 2

X. Class Problem
Presentation of Simple ADP Security Problems and Its Solution
Presentation of Class ADP Security Problem #1 (Let them partially solve in class)

XI. Crypto Principles

XII. Crypto Applications

XIII. Systems Programs

XIV. Machine Architecture

XV. Security Kernels [Software Analysis Tools Micro-processors Security]

XVI. Review Problems

XVII. Review and Micro-processor demonstration

XVIII. Final Examination

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

DODCI SPECIAL/ON-SITE ADP COURSES

Special ADP courses are conducted by the Department of Defense Computer Institute (DODCI) upon written request. Special courses are designed as far as possible to meet the needs of the requesting organization and will be held at DODCI or scheduled on-site. However, if the requesting organization is located in the Washington, D.C. area, the course will be conducted at DODCI where adequate classrooms, support equipment and a computer-based time shared system are readily available.

For special courses the following general guidance is provided to the requesting organizations:

> Subject Matter——Computer fundamentals, computer system development orientation, command and control, information systems analysis and design, ADP resource acquisition, teleprocessing technology, ADP security and computer privacy.

Enrollment should consist of a minimum of 35 and not exceed 45 students. Since DODCI courses are structured at the mid-management level, participation by military (O-1/W-1/E-6 and above) and civil service personnel, GS-9 and above is recommended. To maximize course effectiveness, full-time attendance by students is a prerequisite.

Seven or eight hours of instruction per day will provide for a course length of 3 to 10 days. Based on DODCI experience, a minimum length of 5 days per course is recommended for an effective effort in oreintation courses.

Additional Special Offering:

> SEMINAR in Computer System Security for Senior Executives. This seminar is a one (1) day program on computer system security design to cover the current state-of-the-art in this prominent subject in the world of computing. The seminar will provide senior management personnel with an appreciation for the responsibilities and procedures for the development, management and operation of secure resource-sharing computer systems. Conducted in-house or on-site.

Atch #4

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Charges for DODCI Special/On-Site Courses:

DOD Agencies: No charge is assessed for special courses conducted at the Institute. However, for unprogrammed courses conducted outside the Washington, D.C. area, the requesting command will normally be responsible for funding TDY travel and per diem costs for DODCI instructors assigned. All instructional material, student notebooks and publications will be provided by DODCI. Whenever Federal (non-DOD) employees attend a DOD Agency sponsored course they will be assessed a fee to cover the cost of books and materials. A completed CSC Optional Form 170 will be submitted at enrollment time and subsequently used for billing purposes.

Federal (non-DOD) Agencies: A fee will be assessed to cover the additional expenses incurred on a cost-reimbursable basis. In addition, for on-site courses, the requesting agency will be responsible for reimbursement of total course costs which include instructor salaries, travel and per diem costs plus course material expenses. Exact charges for a specific course can be ascertained by phoning the DODCI Scheduling Office at commercial (202) 433-2020.

To arrange for a special course or a course on-site, a request from the Commanding Officer or the Executive Officer of the requesting agency should be addressed to the Director, DODCI. The letter should cite the objectives to be derived from the course, proposed dates, and the name of a liaison officer within the organization who can be contacted by DODCI for any additional information that may be required.

ADP MANAGERIAL ADVISORY SERVICES

Advisory Services may be arranged at DODCI on written request. These services are necessarily limited by the personnel and facility resouces of the Institute, but frequently, it may be possible to refer activities/organizations needing specialized assistance to competent specialists in other government organizations who can provide the desired advisory service on any specified depth.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

COMPUTER SYSTEM SECURITY	
16 - 19 May 1978	(CS-4-78)
13 - 16 Jun 1978	(CS-5-78)
18 - 21 Jul 1978	(CS-6-78)
15 - 18 Aug 1978	(CS-7-78)
17 - 20 Apr 1979	(CS-7-79)
1 - 4 May 1979	(CS-8-79)
12 - 15 Jun 1979	(CS-9-79)
17 - 20 Jul 1979	(CS-10-79)
14 - 17 Aug 1979	(CS-11-79)
18 - 21 Sep 1979	(CS-12-79)

Atch #5

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

TYPICAL COURSE CONTENT

DEPARTMENT OF DEFENSE COMPUTER INSTITUTE
COMPUTER SYSTEM SECURITY COURSE

Course Introduction. Describes the mission of DODCI and the courses offered. Provides an orientation to DODCI and the surrounding environment. Presents the course objectives and gives the student an overview of the course, and of the realm of computer security concerns that exist today. (1/2 hour)

Analysis of the Computer Security Problem. Presents an overview of specific security problems facing users and managers of ADP systems. Provides a reference for the solutions presented in the balance of the course. (2 hours)

Computer Security Guidance. Reviews the origin, content, and applicability of DOD directives, regulations, and policies as they pertain to the issue of computer security. Reviews service regulations and directives. Also provides an overview of the Privacy Act, Public Law 93-579, and its implementation. (1 hour)

Security Program Development. Describes the requirements for the successful initiation of an ADP security program. Also introduces considerations regarding the value of information and resources, and the requirements for planning, justification, and trade-off analysis. (2-1/2 hours)

Security Program Development Seminar. Provides an opportunity to discuss some of the major problems involved in the development of a successful security program. Case examples are utilized to illustrate recommended techniques for dealing with potential problem areas. (1 hour)

Data Base Integrity. Examines some of the major problems involved in the preservation of data integrity in ADP systems. A variety of technical and administrative integrity safeguards are also discussed. (1 hour)

Computer Resource Protection. Examines the threats against a computer system and evaluates several alternative countermeasures. The essential elements of a computer system safeguards program are examined in detail. (2-1/2 hours)

Software Integrity. Examines recommended procedures for the development, test, and certification of software for secure applications. (1 hour)

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Computer System Security (contd.)

Physical Security and Media Protection. Defines the key elements in a physical security plan. Techniques for the evaluation of physical security hazards are examined in detail. A variety of physical security safeguards which may be utilized to reduce the vulnerability of computer systems are also discussed. (1-1/2 hours)

Data Base Management Systems. Explores the protective features of contemporary data base management systems. (1 hour)

Personnel Security. Discusses some of the typical security problems associated with personnel in an ADP environment and suggests methods of preventing or minimizing the effects of such problems. (1 hour)

The Role of the Auditor. Defines the emerging role of the auditor and his impact upon auditability and the detection of computer abuse. Also provides insight on how the auditor should interface in a computer security program. (1-1/2 hours)

Security Auditing. Defines the various methods of identifying normal and abnormal system activity. Also furnishes guidance regarding the appropriate mix of manual and automated logs required for the security surveillance of an ADP system. (1 hour)

Teleprocessing Network Security. Examines several active and passive threats to teleprocessing systems. Discusses some of the major security considerations involved in intercomputer networks and analyzes a number of countermeasures that may be applied to specific threats. (1-1/2 hours)

Contingency Planning. Provides guidance on the development of a contingency plan, and evaluates some of the advantages and disadvantages of different back-up systems. (1 hour)

Parallel Sessions. Provides an additional opportunity to discuss major problem areas and topics of interest in the area of computer security. (1 hour)

Security Auditing Seminar. Provides an opportunity to discuss solutions to the problems assigned during the Security Auditing lecture. (1 hour)

Safeguards Selection. Analyzes procedures by which the proper mix of available security safeguards can be selected for implementation based upon economic, technical and operational feasibility. (1-1/2 hours)

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Computer System Security (contd.)

Security Program Implementation and Operation. Provides an analysis of the methodology for test, evaluation, implementation and operation of the Computer Security Program. (1 hour)

Security Program Management Seminar. Discusses a variety of considerations regarding the effective management of the Computer Security Program. Also provides a forum for the exchange of student ideas and experiences in dealing with computer security problems. (2 hours)

Course Closing. Summarizes the security course and provides some insight into ADP security developments that can be expected in the future. (1/2 hour)

Last day adjournment approximately 1500 hours.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

EFFECTIVE CS-7-77 (18 - 21 October 1977)

COMPUTER SYSTEM SECURITY COURSE (4 days)

Prerequisites: Officers O-1 and above, Warrant Officers W-1 and above, Enlisted E-6 and above, and Civilians GS-9 and above. Previous attendance at the Introduction to Computer Technology or Computer Orientation for Intermediate Executives courses, or equivalent data processing experience is essential. Attendees should be familiar with their organizations's security procedures and be prepared to discuss security problems during the student seminars. A security clearance is not required for attendance.

Course Content: This course develops an understanding of computer security problems and presents a systematic approach to developing a Computer Security Program. The concepts of risk management, sensitivity analysis, and several analytical techniques for the selection of appropriate safeguards are developed throughout the course. Methodology for test and evaluation, implementation and operation of the Computer Security Program are also discussed.

Who should attend? This course is recommended for ADP managers, computer system users, computer specialists, security officers, or anyone engaged in the management, design, development, procurement, operation, or security of computer systems. The course covers a variety of topics dealing with the protection of data processing resources.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

FY 78/79

TYPICAL CURRICULUM

DEPARTMENT OF DEFENSE COMPUTER INSTITUTE
COMPUTER SYSTEM SECURITY COURSE

TUESDAY

0800 Course Introduction. Describes the mission of DODCI and the courses offered. Provides an orientation to DODCI and the surrounding environment. Presents the course objectives and gives the student an overview of the course, and of the realm of computer security concerns that exist today.

0830 Analysis of the Computer Security Problem. Presents an overview of specific security problems facing users and managers of ADP systems. Provides a reference for the solutions presented in the balance of the course.

1030 Computer Security Guidance. Reviews the origin, content, and applicability of DOD directives, regulations, and policies as they pertain to the issue of computer security. Reviews service regulations and directives. Also provides an overview of the Privacy Act, Public Law 93-579, and its implementation.

1130 LUNCH

1230 Security Program Development. Describes the requirements for the successful initiation of an ADP security program. Also introduces considerations regarding the value of information and resources, and the requirements for planning, justification, and trade-off analysis.

1500 Security Program Development Seminar. Provides an opportunity to discuss some of the major problems involved in the development of a successful security program. Case examples are utilized to illustrate recommended techniques for dealing with potential problem areas.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

WEDNESDAY

0800 Data Base Integrity. Examines some of the major problems involved in the preservation of data integrity in ADP systems. A variety of technical and administrative integrity safeguards are also discussed.

0900 Computer Resource Protection. Examines the threats against a computer system and evaluates several alternative countermeasures. The essential elements of a computer system safeguards program are examined in detail.

1130 LUNCH

1230 Software Integrity. Examines recommended procedures for the development, test, and certification of software for secure applications.

1330 Physical Security and Media Protection. Defines the key elements in a physical security plan. Techniques for the evaluation of physical security hazards are examined in detail. A variety of physical security safeguards which may be utilized to reduce the vulnerability of computer systems are also discussed.

1500 Discussion. Provides an opportunity for student participation in case study analyses.

THURSDAY

0800 Personnel Security. Discusses some of the typical security problems associated with personnel in an ADP environment and suggests methods of preventing or minimizing the effects of such problems.

0900 The Role of the Auditor. Defines the emerging role of the auditor and his impact upon auditability and the detection of computer abuse. Also provides insight on how the auditor should interface in a computer security program.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

1030 Security Auditing. Defines the various methods of identifying normal and abnormal system activity. Also, furnishes guidance regarding the appropriate mix of manual and automated logs required for the security surveillance of an ADP system.

1130 LUNCH

1230 Teleprocessing Network Security. Examines several active and passive threats to teleprocessing systems. Discusses some of the major security considerations involved in intercomputer networks and analyzes a number of countermeasures that may be applied to specific threats.

1400 Contingency Planning. Provides guidance on the development of a contingency plan, and evaluates some of the advantages and disadvantages of different back-up systems.

1500 Parallel Sessions. Provides an additional opportunity to discuss major problem areas and topics of interest in the area of computer security.

FRIDAY

0800 Security Auditing Seminar. Provides an opportunity to discuss solutions to the problems assigned during the Security Auditing lecture.

0900 Safeguards Selection. Analyzes procedures by which the proper mix of available security safeguards can be selected for implementation based upon economic, technical, and operational feasibility.

1030 Security Program Implementation and Operation. Provides an analysis of the methodology for test, evaluation, implementation and operation of the Computer Security Program.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1

1130 LUNCH

1230 Security Program Management Seminar. Discusses a variety of considerations regarding the effective management of the Computer Security Program. Also provides a forum for the exchange of student ideas and experiences in dealing with computer security problems.

1430 Course Closing. Summarizes the security course and provides some insight into ADP security developments that can be expected in the future.

Declassified in Part - Sanitized Copy Approved for Release 2013/01/30 : CIA-RDP89B01354R000200310014-1